Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100 Fax: 623.235.6173

Joseph M. Lyon *(Pro Hac Vice Forthcoming)*
jlyon@thelyonfirm.com
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: 513.381.2333 Fax: 513.766.9011

Terence R. Coates *(Pro Hac Vice Forthcoming)*
tcoates@msdlegal.com
Dylan J. Gould *(Pro Hac Vice Forthcoming)*
dgould@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone 513.651.3700 Fax 513.665.0219

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

JOHN FEINS, individually and on behalf of all others similarly situated, Plaintiff, v. GOLDWATER BANK, N.A. d/b/a, GOLDWATER BANK, Defendant.	Case No.: CV-22-00932-PHX-JJT **AMENDED CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE, AND EQUITABLE RELIEF** **(Jury Demand)**

Plaintiff JOHN FEINS ("Plaintiff") brings this Class Action Complaint against GOLDWATER BANK, N.A. d/b/a Goldwater Bank ("Defendant" or "Goldwater Bank"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal

knowledge as to his own actions, his counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving Goldwater Bank, a domestic for-profit banking institution and mortgage lender.

2. Goldwater Bank failed to reasonably secure, monitor, and maintain the Personally Identifiable Information ("PII") provided by its consumers, including, without limitation, names, addresses, telephone numbers, Social Security numbers, account numbers, and tax identification numbers that were stored on its private network. Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information through their wrongdoing.

3. The full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of the litigation.

4. Moreover, after learning of the Data Breach, Defendant waited roughly six months to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive personal identifying information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

5. As part of its services, Goldwater Bank required its customers, including Plaintiff and Class Members, provide Goldwater Bank with their PII. Plaintiff and Class Members provided Defendant with their PII.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals, and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized access, disclosure, and theft due to criminal hacking

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

activity.

7. In acquiring and maintain Plaintiff's and Class Members' PII, Defendant expressly and impliedly promised to safeguard Plaintiff's and Class Members' PII.

8. Plaintiff and Class Members would not have paid the amounts they paid for Defendant's services, had they known their information would be maintained using inadequate data security systems. Defendant, however, breached their duties, promises, and obligations, and Defendant's failures increased the risk that Plaintiff's PII would be compromised in the event of a likely cyberattack.

9. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable and adequate data security systems and safeguards, including but not limited to a lack of encryption; and/or its failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; and/or its failure to comply with industry-standard data security practices; and/or its failure to comply with state and federal laws and regulations that govern data security and practices and are intended to protect the type of PII at issue in this action.

10. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

11. Criminal hackers obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and the Class Members.

12. As a direct and proximate result of the Data Breach, Plaintiff and Class Members are at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

13. As a direct and proximate result of Defendant's data security failures and the Data Breach, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (v) the invasion of privacy; (vi) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Member's PII; (vii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII; (viii) and the loss of benefit of the bargain for the services that failed to provide reasonable and adequate data security measures.

14. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

15. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

16. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for Negligence (Count I), Invasion of Privacy (Count II), Implied Contract (Count III), Unjust Enrichment (Count IV), and Violations of The New Mexico Unfair Practices Act (Count V).

THE PARTIES

Plaintiff John Feins

17. Plaintiff John Feins is, and at all times relevant has been, a resident and citizen of New Mexico. Plaintiff received a "Notice of Data Breach" letter dated November 1, 2021, on or about that date. The letter notified Plaintiff that on May 21, 2021, Goldwater Bank identified

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

unusual activity on its network and that "hackers were able to gain access to sensitive consumer information." It further stated that Goldwater Bank determined that "an external actor had illegally accessed and/or acquired certain data from the network." The type of data at issue included full names, addresses, Social Security numbers, telephone numbers, account numbers, and tax identification numbers. The letter further advised that Plaintiff should "review your credit reports and account statements over the next 12 to 24 months" for any unauthorized transactions and incidents of suspected identity theft.

18. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff. Plaintiff would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

Defendant Goldwater Bank

19. Defendant Goldwater Bank is an Arizona corporation with its principal office located at 2525 E. Camelback Rd., Suite 1100, Phoenix, Maricopa County, Arizona 85016. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because according to Defendant's Notice of Removal (ECF No. 1), the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

21. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Arizona and this District through its headquarters, offices, parents, and affiliates.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

23. Defendant provides various banking products and services to individuals, including home loans, automobile loans, personal banking, business loans, and home refinancing. It offers online and mobile banking, checking accounts, savings, money market, and wire transfers, as well as certificates of deposit, remote deposit capture, positive pay services, and credit cards. Goldwater Bank further offers business checking, business money market accounts, business savings accounts, cash management and merchant services, business credit cards, and business wire transfers.

24. Plaintiff and Class Members were customers of Defendant whose PII was included in applications and other data submitted to Defendant.

25. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

26. Defendant voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Goldwater Bank has a legal duty to keep consumer's PII safe and confidential.

27. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Goldwater Bank assumed legal and equitable duties and knew or should have

known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach

30. Defendant identified "an attempted ransomware attack" that occurred on May 21, 2021.[1] According to Defendant, it "received alerts of unusual network activity and was able to quickly respond and stop the unauthorized access in process and prevent further infiltration."[2] However, it has not stated when the unusual activity first occurred or how long it took Defendant to realize the attack occurred.

31. Defendant acknowledged that "hackers were able to gain access to sensitive consumer information."[3]

32. Defendant's investigation was inconclusive as to whether or not the accessed data has been or will be misused by the hackers.[4]

33. The attacker accessed, and likely acquired, files on the server containing PII, including names, addresses, telephone numbers, social security numbers, account numbers, and tax identification numbers.

34. On or around October 29, 2021, Defendant also disclosed the Data Breach to the California Attorney General's Office,[5] the Washington State Office of Attorney General,[6] and the Montana Attorney General's Office.[7]

35. Goldwater Bank first notified its impacted consumers of the incident on or around November 1, 2021, sending written notifications to individuals whose personal information was compromised in the Data Breach.

---

[1] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-45.pdf.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] https://oag.ca.gov/ecrime/databreach/reports/sb24-547024.
[6] https://www.atg.wa.gov/goldwater-bank-na.
[7] https://dojmt.gov/consumer/databreach/.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

36. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

37. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

38. In total, Defendant reports that the Data Breach compromised the PII of 11,376 individuals.[8]

39. Defendant has tacitly admitted that the Private Information stolen and subsequently published to the internet was unencrypted. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified the California Attorney General of the Data Breach on or about October 29, 2021, evidencing that the exposed data was unencrypted.[9]

40. To prevent and detect cyberattacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[8] https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Data-Breach-Year-to-date-Report-2021-1.pdf

[9] https://oag.ca.gov/privacy/databreach/list.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

41. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[10]

42. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 11, 2021).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection; and,
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

43. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

44. The occurrence of the Data Breach indicates that Defendant failed to adequately

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

45. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

46. As part of being a customer of Defendant, Plaintiff and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains this information.

47. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

48. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

50. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII.[12]

51. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

52. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class

[12] https://goldwaterbank.com/about/privacy-policy

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Members from being compromised.

Defendant Knew or Should Have Known of the Risk Because the Banking Sector is Particularly Susceptible to Cyber Attacks

53. Defendant knew and understood unprotected or exposed PII in the custody of banking service companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

Value of Personally Identifiable Information

54. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

55. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[13] 17 C.F.R. § 248.201 (2013).
[14] *Id*.
[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 19, 2022).
[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).
[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).

56. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

57. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

58. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2022).

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

impossible, to change—Social Security number, driver's license number, name, and date of birth.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

61. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for years.

63. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

64. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[20] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10xprice-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

67. In the breach notification letter, Defendant made an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

68. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

69. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information, and damage to victims may continue for years.

Defendant Violated the Gramm-Leach-Bliley Act

70. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

71. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

72. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

73. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

74. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous."16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

75. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

76. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

77. The Safeguards Rule, which implements Section 501(b) of the GLBA,15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

78. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

79. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

80. Defendant failed to adequately oversee service providers.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

81. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendant Violated the FTC Act

82. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

83. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Plaintiff John Feins's Experience

84. Plaintiff was required to provide and did provide his PII to Defendant. The PII included his name, address, Social Security number, tax information, employment history, salary information, and information about his bank and brokerage account holdings.

85. To date, Goldwater Bank has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

86. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members' PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

87. Plaintiff and Class Members have been further damages by the compromise of their PII.

88. Plaintiff Feins's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Goldwater Bank's network for the specific purpose of targeting the PII.

89. In December 2021, Wells Fargo notified Plaintiff Feins that a bank account had been opened in his name. Plaintiff Feins did not open an account at Wells Fargo meaning that an unauthorized person opened an account in his name with Wells Fargo.

90. Plaintiff Feins typically takes measures to protect his PII and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

91. Plaintiff Feins stores any documents containing his PII in a safe and secure location. And he diligently chooses unique usernames and passwords for his online accounts.

92. As a result of the Data Breach and subsequent fraud against him, Plaintiff implemented a credit freeze. The implementation of a credit freeze is time consuming and causes substantial inconvenience.

93. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

94. Since the Data Breach, Plaintiff has also experienced a substantial increase in phishing attacks on his email account, including spurious emails purporting to be Wells Fargo. Plaintiff spends significant time reporting these phishing attempts.

95. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

96. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

97. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

98. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he received services from Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

99. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

CLASS ALLEGATIONS

100. Plaintiff brings this suit on behalf of himself and the following classes of similarly situated individuals under Federal Rule of Civil Procedure 23, which are preliminarily defined as:

> **All persons residing in the United States Goldwater Bank, N.A. identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class").**
> **All persons residing in New Mexico Goldwater Bank, N.A. identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Subclass").**

101. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

102. Excluded from the Classes are the following individuals and/or entities:

Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

103. **Numerosity.** The Class and Subclass Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class and Subclass Members are unknown at this time, the identities of Class and Subclass Members are ascertainable through Goldwater Bank's records, Class Members' records, publication notice, self-identification, and other means.

104. **Commonality.** There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Goldwater Bank unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Goldwater Bank failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Goldwater Bank's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Goldwater Bank's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Goldwater Bank owed a duty to Class Members to safeguard their PII;

f. Whether Goldwater Bank breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Goldwater Bank knew or should have known that its data security

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Goldwater Bank's misconduct;

j. Whether Goldwater Bank's conduct was negligent;

k. Whether Goldwater Bank's conduct was per se negligent; and,

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

105. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

106. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

107. **Predominance.** Goldwater Bank has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Goldwater Bank. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties'

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

resources, and protects the rights of each Class member.

109. Goldwater Bank has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

110. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Goldwater Bank owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Goldwater Bank's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Goldwater Bank's failure to institute adequate protective security measures amounted to negligence;

d. Whether Goldwater Bank failed to take commercially reasonable steps to safeguard consumer PII; and;

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

111. Finally, all members of the proposed Class are readily ascertainable. Goldwater Bank has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Goldwater Bank.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

112. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 111 as if fully set forth herein.

113. Goldwater Bank knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

114. Goldwater Bank had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

115. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

116. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

117. Goldwater Bank had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

118. Goldwater had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to A.R.S. §§18-501 – 552.

119. Goldwater Bank, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Goldwater Bank's possession.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

120. Goldwater Bank, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

121. Goldwater Bank, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Goldwater Bank's possession might have been compromised and precisely the type of information compromised.

122. Goldwater Bank's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

123. As a result of Goldwater Bank's ongoing failure to notify Plaintiff and Class Members regarding what type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

124. Goldwater Bank's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

125. As a result of Goldwater Bank's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

126. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

127. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, Goldwater Bank is guilty of oppression, fraud, or malice, in that Goldwater Bank acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

128. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Goldwater Bank to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

129. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 128 as if fully set forth herein.

130. Plaintiff and Class Members maintain a privacy interest in their PII, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

131. Plaintiff and Class Members' PII was contained, stored, and managed electronically in Goldwater Bank's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities.

132. Additionally, Plaintiff's and Class Members' PII, when contained in electronic form, is highly attractive to criminals who can nefariously use their PII for fraud, identity theft, and other crimes without their knowledge and consent.

133. Goldwater Bank's disclosure of Plaintiff's and Class Members' PII to unauthorized third parties as a result of its failure to adequately secure and safeguard their PII is offensive to a reasonable person. Goldwater Bank's disclosure of Plaintiff's and Class Members' PII to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their PII was stored and disclosed private information into the public domain. Plaintiff and Class Members have been damaged by Goldwater Bank's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

134. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 133 as if fully set forth herein.

135. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

136. Plaintiff and Class Members paid money to Defendant and disclosed their PII in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

137. In its written privacy policies, Defendant Goldwater Bank expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances not present here.

138. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

139. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was Defendant's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

140. When Plaintiff and Class Members provided their PII to Defendant Goldwater Bank as a condition of their employment or employee beneficiary status, or as a condition precedent to receiving financial services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

141. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

142. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

143. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

144. Defendant breached their implied contracts with Class Members by failing to safeguard and protect their PII.

145. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

146. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

147. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

148. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 147 as if fully set forth herein.

149. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

150. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

151. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of

reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

152. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

153. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

154. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

155. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

156. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

157. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FIFTH CAUSE OF ACTION
VIOLATIONS OF THE NEW MEXICO UNFAIR TRADE PRACTICES ACT
N.M. Stat. Ann. § 57-12-2, *et seq*.
(on behalf of Plaintiff and the Subclass)

158. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 157 as if fully set forth herein.

159. Defendant knowingly made false and misleading representations and omissions about protecting Plaintiff's and Class Members' PII in connection with financial services,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

including extending credit and loaning money to Plaintiff and Class Members. Defendant's conduct was, and continues to be, in violation of the New Mexico Unfair Trade Practices Act ("UTPA").

160. Defendant Goldwater Bank's representations and omissions that it would protect Plaintiff's and Class Members' personal information were made in the ordinary course of business, trade, and/or commerce.

161. Defendant's privacy policies falsely represented that Defendant would protect personal information from unauthorized access and use, that it used security measures that comply with federal law, that it has implemented computer safeguards and uses secured files and buildings, and that it restricts access to PII to only those employees who need to know such information. Upon information and belief, Defendant provided copies of its privacy policy with these statements to each of its customers and other individuals whose PII it collected. Such statements constitute violations of N.M. Stat. Ann. § 57-12-2 (D)(5), (7), and (14).

162. Defendant separately committed unfair and deceptive acts and practices in violation of the UTPA by omitting from Plaintiff and the Class that it failed to implement and maintain reasonable security measures to safeguard PII. Defendant should have disclosed these failures to Plaintiff and the Class before obtaining their PII. Had Plaintiff and the Class known of Defendant's failures, they would not have entrusted Defendant with their PII.

163. Defendant's violations of the UTPA are further supported by federal law. *See* N.M. Stat. Ann. § 57-12-4 ("It is the intent of the legislature that in construing Section 3 of the Unfair Practices Act the courts to the extent possible will be guided by the interpretations given by the federal trade commission and the federal courts."). The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an unfair practice in violation of the Federal Trade Commission Act. *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244-247 (3d Cir. 2015); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F.Supp.3d 1295, 1327-1328 (N.D. Ga. 2019).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

164. Defendant's misrepresentations and omissions were material and the type that tend to, do, and did deceive Plaintiff and Class Members, especially considering that Defendant was not adequately protecting and ultimately failed to protect Plaintiff's and Class Members' personal information.

165. Plaintiff and Class Members have been damaged, and are at an imminent and substantial risk of future harm, as a result of Defendant's conduct, representations, and omissions in violation of the UTPA.

166. Plaintiff and the Class Members are entitled to statutory and actual damages, injunctive relief, and attorneys' fees as a result of Defendant's UTPA violations.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

RESPECTFULLY SUBMITTED this 6th day of July, 2022.

PEREZ LAW GROUP, PLLC

/s/ *Cristina Perez Hesano*
Cristina Perez Hesano, Esq.
Attorney for Plaintiff

Joseph M. Lyon (*pro hac vice* forthcoming)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Terence R. Coates (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff and the Class

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301